REMARKS

Claims 1-33 are currently pending in the subject application and are presently under consideration. Claims 1, 2, 9, 15, 20, 23-25, and 27-29 have been amended to further emphasize aspects which applicants' claim as the invention as shown at pages 2 to 7 of the Reply.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claims 1-8 and 11-33 Under 35 U.S.C. §103(a)

Claims 1-8 and 11-33 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Flowers, *et al.* (US 6,957,348) in view of Brown (US 6,571,141). It is requested that this rejection be withdrawn for at least the following reasons. Flowers, *et al.* and Brown taken alone or in combination do not teach or suggest every element of the claimed invention, and further, one ordinarily skilled in the art could not combine these references to successfully implement the claimed invention.

> To reject claims in an application under §103, an examiner must establish a *prima facie* case of obviousness. A *prima facie* case of obviousness is established by a showing of three basic criteria. First, there ***must be some suggestion or motivation***, either in the references themselves or in the knowledge generally available to ***one of ordinary skill in the art, to modify the reference or to combine reference teachings***. Second there must be a ***reasonable expectation of success***. Finally, the prior art reference (or references when combined) ***must teach or suggest all the claim limitations***. *See* MPEP §706.02(j). The ***teaching or suggestion to make the claimed combination*** and the reasonable expectation of success ***must be found in the prior art and not based on the Applicant's disclosure***. *See In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991) (emphasis added).

The subject invention generally relates to a system that automates security in an industrial control environment by automatically creating security profiles for industrial automation devices in the environment and enforcing these profiles with respect to accessing entities. Such profiles may define different levels of access for various entities. To this end, independent claim 1 (and similarly independent claims 28 and 29) recites an asset component that defines an ***industrial automation device***, an access component that ***defines a security attribute*** associated with the

industrial automation device, and a security component that ***regulates access to the industrial automation device based upon the security attribute***. Flowers, *et al.* and Brown, when taken alone or in combination, fail to teach or suggest every element of the claimed invention.

Flowers, *et al.* generally relates to allowing a vulnerability detection system and an intrusion detection system, for conventional networked computer environments, to interoperate with each other such that the intrusion detection system can utilize information received from the vulnerability detection system to choose areas for monitoring. (*See* col. 1, line 18 to col. 2, line 60). Another aspect of the cited reference is to ease the use and configuration of such components for a systems engineer. Accordingly, the vulnerability detection portion of the system is able to interrogate other systems on the network to determine potential weaknesses within the system. The data gathered from this component is stored with a way to cure the weakness, and the intrusion detection system may utilize this information for its subsequent operations. However, Flowers, *et al.* is silent regarding defining an ***industrial automation device***.

Contrary to the claimed invention, the system of Flowers, *et al.* interfaces with computers and servers in a conventional computer network and not industrial devices. (*See* col. 3, ll. 30-32). Industrial devices differ from conventional computers in that they employ proprietary protocols and often require specialized hardware and/or software to facilitate communication with convention computers. Unlike the system of Flowers, *et al.*, the claimed invention is operable in an industrial controller environment wherein such proprietary industrial automation devices exist. Specifically, the security component of the claimed invention can access the various PLCs and industrial automation devices to gain type information and accordingly create security profiles based on this information. This functionality of defining an ***industrial automation device*** is specific to a system operable in industrial controller environments such as the claimed invention. The system disclosed in Flowers, *et al.* would not be operative in such an environment to achieve the foregoing ends since the system is disclosed as merely operating in the conventional computer network environment. Thus, Flowers, *et al.* fails to disclose this aspect of the claimed invention.

Furthermore, the Examiner contends that Flowers, *et al.* discloses defining one or more vulnerabilities associated with a network resource. Applicants' representative avers to the contrary at least on the ground that vulnerabilities are not attributes. It is to be appreciated that

an attribute is used to describe a parameter or property of an entity associated with a value, whereas a vulnerability indicates a place in a system where security may be lacking. Specifically, a vulnerability lacks the tangibility of an attribute. Attributes are descriptive in nature, whereas a vulnerability is associated with a weakness in a system. It is apparent that Flowers, *et al.* further fails to disclose ***defining a security attribute*** associated with the industrial automation devices.

The Examiner acknowledges that Flowers, *et al.* does not disclose ***regulating access to the industrial automation device based upon the at least one security attribute*** and offers Brown to cure this deficiency. However, Brown also fails to disclose this aspect. More specifically, Brown relates to API access and parameter blocking such that software application designers implementing programs for motion control systems may be limited to the types of functions they can access as well as the scale of parameters they can specify. Therefore, Brown relates to regulating access of software application programmers at program design and implementation time within a given system. Brown does not disclose ***regulating access to the industrial automation device based upon the at least one security attribute***.

In particular, Brown does not teach controlling access to motion control systems *including* restricting access to one or more API functions, rather, the system in Brown is actually *limited* to restricting access to one or more API functions. The claimed invention, however, regulates access to the factory asset as a whole regardless of whether an API is present, and therefore is not bound by requiring an API in the first place as in Brown. For at least these reasons, Brown does not teach the subject invention as recited in the claims, nor does it cure the deficiencies of Flowers, *et al.*

Additionally, the operating environment disclosed in Brown is within a computer that accesses attached mechanical devices through directly connected interface cards. The environment of the subject invention, however, is a networked industrial control environment, as understood by those having ordinary skill to comprise industrial controllers existing at disparate locations and not limited to being accessed by a single entity as disclosed in Brown. In view of this, one ordinarily skilled in the art would not seek to utilize Brown to create the subject invention.

Moreover, one having ordinary skill in the art would not seek to combine the systems of Flowers, *et al.* and Brown – as Brown deals with a system that controls mechanical devices

through controller cards and Flowers, *et al.* relates to detecting vulnerabilities and intrusions with respect to servers participating in a computer network. Stated differently, Brown is only operable with respect to motion control systems, and Flowers, *et al.*, as shown above, cannot be utilized in such a system and vice versa. For at least the foregoing reasons, rejection of claims 1, 28 and 29 (and claims 2-8, 11-19, and 30-33 which depend therefrom) should be withdrawn.

Claim 20 of the subject invention recites ***a security management module . . . for enforcing an enterprise wide policy and to manage security threats directed to networked industrial automation devices***. Flowers, *et al.* and Brown fail to teach or suggest such claimed aspects as well.

The Examiner provides Brown to cure the deficiencies of Flowers, *et al.* related to this aspect; however, as discussed *supra*, Brown generally relates to a system to block API functions and limit parameters of such functions in a computer that controls mechanical devices. Brown does not disclose operability in networked factory asset systems (or networked industrial controller environments) meaning it cannot be said to disclose ***managing security threats directed to networked industrial automation assets***. Furthermore for this reason, and since Brown is otherwise silent, Brown does not disclose ***enforcing an enterprise wide policy*** since enforcing such a policy implies operating in a networked enterprise environment wherein the policy is defined centrally and enforced throughout the network as understood by one having ordinary skill in the art. For at least the foregoing reasons, Brown fails to make up for the aforementioned deficiencies of Flowers, *et al.* with respect to claim 20, and rejection of this claim (and claims 21-23 which depend therefrom) should be withdrawn.

Similarly, claim 24 recites ***developing a security framework for an automation system based in part on the modeling of the industrial automation devices and a network access type***. Flowers, *et al.* and Brown are also silent with regard to such claimed aspects.

Modeling automation assets in the claimed invention involves automatically defining security profiles for a given industrial controller based on at least one security attribute. The Examiner asserts that Flowers, *et al.* does not disclose this aspect and offers Brown to overcome this omission. However, Brown is silent regarding this functionality; as well, Brown is silent with regard to networked components such that the security framework in Brown does not depend on any ***network access type***. For this reason, Brown fails to make up for the omissions of Flowers, *et al.*, and therefore, rejection of claim 24, as well as claims 25-27 which depend

therefrom should be withdrawn. Since it has been shown that rejection of all independent claims under 35 U.S.C. §103(a) is improper over Flowers, *et al.* and in view of Brown, rejection of these claims and all associated dependent claims should be withdrawn.

II. Rejection of Claims 9-10 Under 35 U.S.C. §103(a)

Claims 9-10 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Flowers, *et al.* (US 6,957,348) in view of Brown (US 6,571,141) and further in view of Blumenstock, *et al.* (US 2002/0006790). It is requested that this rejection be withdrawn for at least the following reasons. Flowers, *et al.*, Brown, and Blumenstock, *et al.*, taken alone or in combination do not teach or suggest every element of the claimed invention. More specifically, Blumenstock, *et al.* fails to make up for the aforementioned deficiencies or Flowers, *et al.* and Brown with respect to independent claim one, from which claims 9-10 depend. Therefore, this rejection should be withdrawn.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [ALBRP303USA].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,

AMIN, TUROCY & CALVIN, LLP

/Himanshu S. Amin/
Himanshu S. Amin
Reg. No. 40,894

AMIN, TUROCY & CALVIN, LLP
24TH Floor, National City Center
1900 E. 9TH Street
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731